УДК 37.022

ИНТЕГРАЦИЯ ОБУЧЕНИЯ МАТЕМАТИКИ И ИНФОРМАТИКИ ПРИ ИЗУЧЕНИИ ТЕОРИИ ЧИСЕЛ

Бушмелева Н.А., кандидат педагогических наук, доцент,
Вятский государственный университет, г. Киров
na_bushmeleva@vyatsu.ru

Разова Е.В., кандидат педагогических наук, доцент,
Вятский государственный университет, г. Киров
ev_razova@vyatsu.ru

Аннотация. В работе приводится иллюстрация интегративного подхода математической подготовки бакалавров при организации обучения теории чисел, который заключается в построении и анализе математических моделей и построении алгоритмов при решении задач теории чисел.

Ключевые слова: интегративный подход в обучении, обучение математике в вузе.

INTEGRATION OF THE TEACHING OF MATHEMATICS AND COMPUTER SCIENCE IN THE STUDY OF NUMBER THEORY

N.A. Bushmeleva, candidate of pedagogical sciences, associate professor,
Vyatka State University, Kirov
na_bushmeleva@vyatsu.ru

E.V. Razova, candidate of pedagogical sciences, associate professor,
Vyatka State University, Kirov
ev_razova@vyatsu.ru

Abstract. The work illustrates the integrative approach of mathematical training of bachelors in the organization of training in number theory, which consists in the construction and analysis of mathematical models and the construction of algorithms for solving problems in number theory.

Keywords: integrative approach in teaching, teaching mathematics in higher education.

Современный этап развития общества характеризуется стремительным увеличением объема информации и развитием средств информационных и коммуникационных технологий, используемых во многих областях деятельности человека. С постоянно возрастающим объемом информации важно сформировать у обучающихся навыки работы с информацией такие, как поиск, систематизация, анализ. Поэтому особую значимость приобретают информатизация и фундаментализация образования. Их следует рассматривать как целенаправленно организованный процесс обеспечения сферы образования методологией, технологией и практикой создания и оптимального использования методик, ориентированных на реализацию научно-методических и практических основ фундаментального образования и на использование возможностей информационных и коммуникационных технологий.

Современному студенту важно понимать значимость получаемых им знаний, важно иметь ответ на вопрос о необходимости изучать тот или иной курс предметной подготовки. Современное образование должно быть нацелено на новые ориентиры профессиональной реализации, должно быть изменено представление о целях и ценностях образования, требуется пересмотр содержания подготовки. Возникает необходимость повышения уровня межпредметных знаний, в частности в области математики и информатики. Методическая система интегрированного изучения математики и информатики приобретает в современных условиях принципиально новое значение. Такой подход должен позволить показать практическую значимость классических разделов «чистой» математики, ее роль в развитии других областей науки.

Одним из таких разделов классической математики является теория чисел, изучение которого включено в образовательные программы многих направлений подготовки информационного,

технического и математического профилей. В учебниках и учебных пособиях для вузов по теории чисел [1, 2, 4, 5] традиционно находят свое отражение следующие разделы:

1. Теория делимости в кольце целых чисел

Делимость целых чисел, свойства делимости. Теорема о делении с остатком. Общий делитель, наибольший общий делитель (НОД), свойства НОД. Алгоритм Евклида. Теорема о линейном разложении НОД. Наименьшее общее кратное (НОК), свойства НОК. Взаимно простые числа, свойства взаимно простых чисел.

2. Простые и составные числа. Основная теорема арифметики

Простые и составные числа, свойства простых чисел. Основная теорема арифметики. Описание делителей натурального числа. Количество $\tau(n)$ и сумма $\sigma(n)$ делителей натурального числа. Каноническое разложение натуральных чисел. Нахождение НОД и НОК с помощью канонических разложений. Теорема Евклида. Теорема об интервалах. Решето Эратосфена. Важнейшие функции в теории чисел: $[x]$ и $\{x\}$ их свойства**.**

3. Мультипликативные функции и их примеры

Мультипликативные функции и их свойства. Примеры мультипликативных функций: число делителей данного числа, сумма делителей, функция Мебиуса, функция Эйлера.

4. Цепные дроби

Цепные дроби. Разложение рациональных чисел в цепную дробь. Подходящие дроби, вычисление подходящих дробей, переход от цепной дроби к неправильной. Свойства подходящих дробей. Полное и неполное частные подходящих дробей. Разложение иррациональных чисел в цепную дробь. Периодичность бесконечной цепной дроби. Приближение иррациональных чисел подходящими дробями.

5. Теория сравнений

Отношение сравнимости по модулю и его основные свойства. Классы вычетов по данному модулю, свойства классов вычетов. Кольцо Z_n,поле Z_p и группа Z_n^*. Делители нуля в кольце классов вычетов. Полная и приведенная система вычетов. Мультипликативная группа обратимых элементов. Теорема Эйлера и малая теорема Ферма. Тождество Гаусса.

6. Сравнения 1-ой степени

Сравнения первой степени и их решение. Неопределенные уравнения. Системы сравнений. Решение систем сравнений. Китайская теорема об остатках. Теорема Вильсона. Сравнения высшей степени по простому модулю. Сравнения по составному модулю. Показатель класса.

7. Первообразные корни и индексы. Двучленные сравнения

Первообразные корни, теоремы о существовании первообразных корней. Индексы, таблицы индексов. Теоремы о первообразных корнях и индексах. Двучленные сравнения по простому модулю. Вычет n-ой степени по простому модулю. Теорема о числе классов вычетов.

8. Сравнения 2-ой степени

Квадратичные вычеты и невычеты. Сравнения 2-ой степени по простому модулю. Символ Лежандра, свойства символа Лежандра. Критерий Эйлера. Закон взаимности. Символ Якоби, свойства символа Якоби. Сравнения 2-й степени по составному модулю

9. Дискретное логарифмирование

Логарифмирование в конечных полях. Примеры логарифмирования в конечных полях. Сложность алгоритмов логарифмирования в конечных полях.

Материал курса «Теория чисел» концентрирует в себе достаточно большой теоретико-числовой материал и богатую алгоритмическую составляющую. Методы информатики применяются здесь для эффективного решения задач теории чисел и ее приложений. На основе проведенного анализа теоретического материала и его приложений, выявлена его алгоритмическая составляющая:

- алгоритмы «длинной» арифметики;
- алгоритм Евклида;
- расширенный алгоритм Евклида;
- алгоритм разложения числа в цепную дробь;
- тесты проверки простоты числа (решето Эратосфена, тест на основе малой теоремы Ферма, свойства чисел Кармайкла, тест Рабина-Миллера и др.);

– генерация простых чисел (решето Эратосфена, алгоритмы построения больших простых чисел (числа Мерсена и др.));

– алгоритмы разложения числа на множители (факторизация числа);

– алгоритмы возведения числа в степень;

– алгоритмы решения линейных диофантовых уравнений;

– алгоритмы решения сравнений, систем сравнений;

– алгоритмы дискретного логарифмирования.

Кроме того, теоретико-числовой материал является фундаментом для решения таких задач информатики, как построение методов защиты информации [3]. В частности можно выделить следующие приложения теории чисел в криптографии:

– шифрование с открытым ключом (например, схема RSA);

– криптографические протоколы (например, системы Диффи-Хеллмана и Эль-Гамаля);

– электронно-цифровая подпись (например, алгоритм DSA);

– аутентификация и идентификация (например, схема Клауса Шнорра, аутентификация на основе алгоритма RSA, схема Фейге-Фиата-Шамира).

Таким образом, изучение теории чисел, основанное на интеграции с вопросами и дисциплинами компьютерной подготовки, позволяет расширить базу задач и алгоритмов, позволяет продемонстрировать практическую значимость классического математического знания. При этом изучение теории чисел должно происходить с применением инновационных для математики, основанных на информатизации средств. Обучающиеся должны не только научиться решать математические задачи, но и уметь отобрать средства для их решения. При решении математических задач при изучении теории чисел необходимо уделять внимание не только чисто математическому решению, но и компьютерному моделированию теоретико-числовых задач, вопросам возможности реализации алгоритмов решения задач, поиску наиболее эффективных алгоритмов.

Именно программирование, представляющее собой деятельность, которая в узком смысле сводится к кодированию рассматриваемого алгоритма, а в широком является методологией информатики, то есть вычислительным экспериментом, должно стать средством организации обучения «Теории чисел». Оно открывает большие возможности для расширения круга решаемых задач, поскольку позволяет использовать в обучении, во-первых, задачи, требующие значительных вычислительных затрат для их решения, во-вторых, задачи, требующие использования комбинаторных методов решения.

Движущая сила образовательного процесса состоит в противоречии между теми задачами, которые ставятся перед студентом и его знаниями, умениями и навыками. Самостоятельная деятельность по устранению этого противоречия является залогом повышения качества обучения. Программирование как средство организации обучения при изучении курса стимулирует активность и самостоятельность обучающихся, способствует их развитию через преодоление собственных ошибок благодаря постоянной обратной связи, поддерживаемой компьютером. Оно способствует большей осознанности изучаемого теоретического материала, поскольку требует от студентов четкости в формализации используемого материала, точности в выражении своих мыслей и т.п. Построение математической модели прикладной задачи, разработка и обоснование алгоритма, его программная реализация и исследование позволяют сформировать навыки компьютерного моделирования, организации и проведения вычислительного эксперимента.

Построенная таким образом система обучения дисциплине «Теория чисел»:

– обеспечивает интеграцию математики и информатики;

– усиливает межпредметные связи изучаемого курса с другими науками, и имеет высокую прикладную направленность;

– способствует формированию представления о роли и месте математики, обеспечивает демонстрацию применения компьютерных технологий при исследовании математических задач;

– повышает математическую культуру учащихся;

– способствует привитию практических навыков математического моделирования и вычислительного эксперимента как инструментов учебной, научно-исследовательской и практической деятельности.

Интеграция математики и информатики при построении системы обучения дисциплине «Теория чисел» несет в себе огромный образовательный потенциал. Позволяет повысить математическую и алгоритмическую культуру, привить устойчивый интерес к математике через показ красоты, как самой математической теории, так и эффективное решение с помощью компьютера конкретных проблем теории чисел и ее приложений.

Литература

1. Бухштаб А.А. Теория чисел / А.А. Бухштаб. – М.: Просвещение, 1966. – 383 с.
2. Виноградов И.М. Основы теории чисел / И.М. Виноградов; под ред. А.Э. Рывкина. – Изд. 6-е, испр. – Москва-Ленинград: Государственное издательство технико-теоретической литературы, 1952. – 181 с.
3. Кнауб Л.В. Теоретико-численные методы в криптографии: учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. – Красноярск: Сибирский федеральный университет, 2011. – 160 с.
4. Манин Ю.И. Введение в современную теорию чисел / Ю.И. Манин, А.А. Панчишкин. – М.: МЦНМО, 2009. – 552 с.
5. Сизый С.В. Лекции по теории чисел: учебное пособие / С.В. Сизый. - 2-е изд., испр. – М.: Физматлит, 2008. – 191 с.